Exhibit A

Observations from Hart/Intercivic evaluation

J. Alex Halderman <halderman@gmail.com> Tue, Jan 29, 2019 at 10:43 AM
To: "Kotula, Kathleen" <kkotula@pa.gov>, "Hartzell, John" <johhartzel@pa.gov>
Bcc: "Ilann M. Maazel" <imaazel@ecbalaw.com>

Hi Kathy and John,

Thanks to both of you and to the rest of the elections staff for accommodating me this week in Harrisburg. I've written up some preliminary observations and suggestions based on what I saw during the tests. Most of my feedback concerns issues that I think warrant further testing, but there are also some items that I hope you will take into consideration while making certification decisions and crafting procedural requirements.

Certainly some of these issues are shared by other vendors' systems, and I hope to have a chance to go back and review the videos from those tests so I can provide similar feedback. Please let me know how I can get access to those videos.

If I missed something or got some detail wrong, I'd be grateful for clarification. I'd also be happy to further discuss my concerns if that would be helpful.

Best regards,

Alex

Auditability

Complex computer voting systems will inevitably have security vulnerabilities, and the best we can do with available technology is raise the bar for attacks. For this reason, one of my primary concerns with any new voting system is whether it supports rigorous post-election audits, which are the best technology we have for detecting and correcting outcome-altering error or fraud.

- **I have serious concerns about whether the Verity Print BMD system can support rigorous post-election audits. Although the machine produces a voter-verifiable record, the printout is a summary ballot that is awkwardly formatted, hard to quickly interpret, and difficult for voters to associate with the full set of races and candidates from which they make their selections. I'm concerned that many voters will overlook errors in these printouts.**

The ballot includes a column with party affiliations of the selected candidates, which is relatively easy for a voter to scan for errors. I'm more worried about down-ballot races for which there are multiple candidates from the same party, and about ballots where the voter has selected a few candidates from each party.

Suppose only 10% of voters spot errors; sufficient fraud to flip the outcome of a close race with a 1% margin of victory would result in only about one error report per precinct—which poll workers might naturally ascribe to user error on the voter's part. If BMDs are to serve as the basis for a rigorous audit, they need to be designed and tested for usability to ensure that the probability of errors getting detected is high. There should also be procedures to encourage voters to check for errors and require poll workers to carefully track error reports during voting. Absent these safeguards, the paper ballots don't provide robust protection.

Software Updates

- **The Verity servers and polling place equipment run on Windows (in kiosk mode?). What version of Windows is it? What provisions are in place to promptly update Windows as vulnerabilities are found? What provisions are in place to ensure that updates continue for the lifespan of the equipment?**

Prompt OS updates are especially important for the Verity system, because it relies on USB connections for distributing ballots, tabulating results, authenticating officials, attaching to external scanners and printers, and exporting data from servers. USB is a complex protocol managed by the operating system, and it has a larger attack surface than other data media, such as memory cards. Novel vulnerabilities in the Windows USB subsystem have been used in the past to spread malware created by nation-states. Note that the Verity back-office system computers all had unsealed USB ports, and the design necessitates leaving these ports accessible.

Windows security updates are typically released once a month on the second Tuesday (timing that, inconveniently, sometimes falls on the day of a general election). The vendor should have procedures in place to promptly certify and deliver any applicable updates, and municipalities should have procedures in place for promptly installing them. The cost of such updates and their installation should be factored into the lifetime

cost of the system. As for any election equipment, I urge the state to require municipalities to use the most up-to-date approved version of all software and firmware.

- **What is the process for installing software updates? Can it be carried out by third-party service personnel, or only by the manufacturer? How are updates authenticated? Is there an adequately secured process for updating BIOS firmware and Windows, in addition to the election application software?**
Poorly designed software update mechanisms have led to severe vulnerabilities in other U.S. voting systems. Software updates will almost certainly be necessary over the lifetime of the system to correct problems at all layers of the software stack. Since updates are such an important part of the system's lifecycle, I suggest covering them in future public tests—there was no mention this week.

Firmware in COTS Devices

- **Verity configurations contain several security-relevant COTS components, including the ballot printer (an Oki B432), central-count scanner (a Cannon DR-G1100), and USB duplicator (a VINPower USBShark). All contain upgradable firmware that, if vulnerable or compromised, could interfere with election processes. For instance, malicious firmware in the scanner could alter the scanned images to show marks for difference candidates. I and colleagues demonstrate such an attack in a forthcoming research paper.**
These three devices are designed to have their firmware updated via USB interfaces, which must be left accessible in order to attach them to the other Verity components. Based on public documentation, only the printer seems to allow users to set an administrative password to control the installation of new firmware. Testing should ensure that this password has been changed from the default ("aaaaaa"). There should be procedures for updating the firmware in these devices if security patches become available.

Voter Privacy

- **Verity systems printed unique code numbers and barcodes on each ballot. These use an alphanumeric encoding, and they seemed to reflect the time that the ballot was printed (as a counter incrementing every second). Is this correct? Can this behavior be disabled?**

Printing a timestamp on the ballots raises significant privacy concerns, since an attacker who notes who cast ballots on what machines when (such as an observer positioned by a candidate) could associate each voter with their ballot during a recount. PA election statutes appear to require paper ballots *not* to contain distinguishing marks, with serial numbers printed only on detachable stubs.

- **In addition to the unique codes mentioned above, the Verity Print BMD produces a QR code on each summary ballot. It's unclear whether this QR code can also be used to uniquely identify the ballot.**
The QR code decodes to a roughly 440-bit random-looking sequence, which may be a digital signature of the ballot contents. It's possible to construct a signature that doesn't convey any information beyond the integrity of the ballot choices, but it's also possible to construct signatures that uniquely track each individual ballot--and hence could compromise privacy.

- **The Verity Print BMD has an integrated printer that produces summary-style paper ballots. Unlike the external printer used by Verity Touch Writer, the integrated printer produces audible mechanical noises that seem to correlate with the content being printed. It's likely that the voter's ballot selections (at least the length of the chosen candidate name in each race) can be determined from the printer's sound—almost certainly with a simple mobile app, and perhaps even by a trained listener.**
I may ask a student to attempt to build such software as a demonstration using the audio recording from the test video. This is an example of a *side-channel*—a class of information leakage vulnerabilities. Another possible side-channel is the accessibility devices used with Verity Touch Writer: the headphones, at least, appeared to have an unshielded cable, which risks leaking radio-frequency signals that could be picked up at a distance with a low-cost receiver.

- **In at least one configuration, the ballot printer can scan a barcode produced by an e-pollbook to select the appropriate ballot style. Voters might believe—or be fooled into believing—that their identity gets associated with their ballot choices based on these barcodes.**
To avoid such a risk, it's good practice to separate the voter check-in system from the ballot casting and scanning system.

- **The voter's ballot selections are *clearly* visible to an observer standing at least 15 feet behind the voter and slightly to the left.** I note this primarily because the video narration gave a different impression. Poll workers should carefully protect this line of sight.

- **The audio ballot recording was *clearly* audible across the testing room when the headphone volume was increased sufficiently above the default level. This is concerning for voters who have both visual and auditory impairments and might require a high audio level.**

Key Distribution

- **Verity relies on cryptographic keys to digitally sign and authenticate election data, as well as (apparently?) to sign the summary ballot via the QR code. A cryptographic secret is presumably also used to authenticate vKeys. How are these signing keys and other secrets distributed to election system components? Can they be changed, or are they the same across all Verity installations?**
  Shared or unchangeable cryptographic keys have been a source of severe vulnerabilities in other U.S. voting systems. Using the same key over a wide area or across jurisdictions leads to a large attack surface; an attacker who can successfully compromise any of the systems that share the secret key can extract it and use it to attack the others. I suggest covering key distribution processes in future public tests—they were entirely omitted this week.

Authentication

- **The Verity system uses a USB key called a "Verity Key" or "vKey", along with a secret PIN, as a two-factor authentication mechanism. (The vKey is actually an iButton device in a COTS USB adapter.) Two-factor authentication is a good practice, but the factors need to be well designed. Does the system strongly protect against attempts by an attacker who acquires a vKey to discover the PIN by brute force? Is this true even if the attacker attaches a vKey to hardware and software he controls?**
  During testing, an incorrect PIN appeared to result in an immediate error message, which implies that guessing attacks may not be velocity limited. If this is true (and assuming that the guessing process could be automated), brute forcing a 6- or 8-digit PIN would be very fast, given access to the vKey.

Physical Security

- **In general, I don't think security seals provide much value—research has shown that most widely used seals can be defeated with simple techniques and readily available tools. However, even assuming that the seals *do* work as intended, the physical security demonstration raised several concerns:**
  - **Is it possible to pry off the plastic door covering the vDrive and vKey access ports?** It's only sealed from the front, and the thin plastic might be flexible enough to bend and disengage the plastic tabs in the rear.
  - **Can the machine casing, when sealed with a wire around the front handle, be opened by removing the hinge in the rear?** It looked like the hinges might be attached with externally facing screws, and there appears to be nothing preventing the pins from being removed from the hinges while the case is closed.
  - **The locks appeared to be of a low quality type that would be easy to pick open.** I found one of the keys available for purchase on the Internet by Googling the code printed on it.

J. Alex Halderman <halderman@gmail.com> Thu, Feb 21, 2019 at 2:44 PM
To: "Kotula, Kathleen" <kkotula@pa.gov>, "Hartzell, John" <johhartzel@pa.gov>
Bcc: "Ilann M. Maazel" <imaazel@ecbalaw.com>

Hi Kathy and John,

I'm writing again to confirm that you received the observations I sent last month, and to ask again how I can obtain the videos from your earlier certification sessions. I'd like to review them.

Thanks in advance for your help.

Alex
[Quoted text hidden]

Kotula, Kathleen <kkotula@pa.gov> Tue, Feb 26, 2019 at 10:13 PM
To: "J. Alex Halderman" <halderman@gmail.com>, "Hartzell, John" <johhartzel@pa.gov>

Dr. Halderman –

Thanks for following up with us. We did receive your email last month and shared your comments with our agency client. Regarding the videos, we have to work with the vendors first to review the videos for proprietary information.

Thanks again,

Kathleen

From: J. Alex Halderman <halderman@gmail.com>
Sent: Thursday, February 21, 2019 2:45 PM
To: Kotula, Kathleen <kkotula@pa.gov>; Hartzell, John <johhartzel@pa.gov>
Subject: [External] Re: Observations from Hart/Intercivic evaluation

ATTENTION: *This email message is from an external sender. Do not open links or attachments from unknown sources. To report suspicious email, forward the message as an attachment to CWOPA_SPAM@pa.gov.*

[Quoted text hidden]

J. Alex Halderman <halderman@gmail.com> Tue, Feb 26, 2019 at 10:20 PM
To: "Kotula, Kathleen" <kkotula@pa.gov>
Cc: "Hartzell, John" <johhartzel@pa.gov>

I appreciate the reply. Do you know when the videos will be available?
[Quoted text hidden]

J. Alex Halderman <halderman@gmail.com> Tue, Feb 26, 2019 at 10:29 PM
To: "Kotula, Kathleen" <kkotula@pa.gov>
Cc: "Hartzell, John" <johhartzel@pa.gov>

Also, weren't these certification sessions done in public? I'd just like to see what the public already saw, since I wasn't there at the time.

Many thanks,

Alex
[Quoted text hidden]

J. Alex Halderman <halderman@gmail.com> Thu, Mar 7, 2019 at 10:21 AM
To: "Kotula, Kathleen" <kkotula@pa.gov>
Cc: "Hartzell, John" <johhartzel@pa.gov>

Hi Kathy, John,

I'm writing again to ask when the other videos will be available for review. Since many counties are looking to purchase machines, and their decisions might be better informed by public feedback, time is of the essence.

Thanks,
Alex
[Quoted text hidden]

Hartzell, John <johhartzel@pa.gov> Fri, Mar 8, 2019 at 4:43 PM
To: "J. Alex Halderman" <halderman@gmail.com>, "Kotula, Kathleen" <kkotula@pa.gov>

Alex:

Good afternoon. We are providing an opportunity to the vendors to take a look at the videos to ensure there was no proprietary or confidential information, or trade secrets, disclosed as part of the evaluations. While the certifications were undertaken in a public setting, there was no public or competitors present. Therefore, the reality of the demonstrations may have resulted in sharing of information beyond what was needed for the certification.

We understand your desire to have access to the videos at the earliest opportunity. As soon as we have details on the timing of access we will be in touch. Thanks.

Regards,

John

John M. Hartzell | Deputy Chief Counsel

PA Department of State | Office of Chief Counsel

306 North Office Building | Harrisburg, PA 17120

Phone: 717.857.3619 | Fax: 717.214.9899

www.dos.state.pa.us

[Quoted text hidden]

J. Alex Halderman <halderman@gmail.com> Thu, Mar 28, 2019 at 12:03 PM
To: "Hartzell, John" <johhartzel@pa.gov>
Cc: "Kotula, Kathleen" <kkotula@pa.gov>

Hi John,

Any update on the status of the videos?

Would it be possible to at least get the video from the Hart certification now, since I was present in person while that was filmed?

Best,
Alex
[Quoted text hidden]

J. Alex Halderman <halderman@gmail.com> Wed, Apr 17, 2019 at 9:22 PM
To: "Hartzell, John" <johhartzel@pa.gov>
Cc: "Kotula, Kathleen" <kkotula@pa.gov>

Hi John and Kathy,

Any updates about when the videos might be available? I asked almost three months ago. It would be helpful even to get the Hart video, from the session where I was present.

Thanks,
Alex
[Quoted text hidden]